

Fig. 1A (Prior Art)

2/73

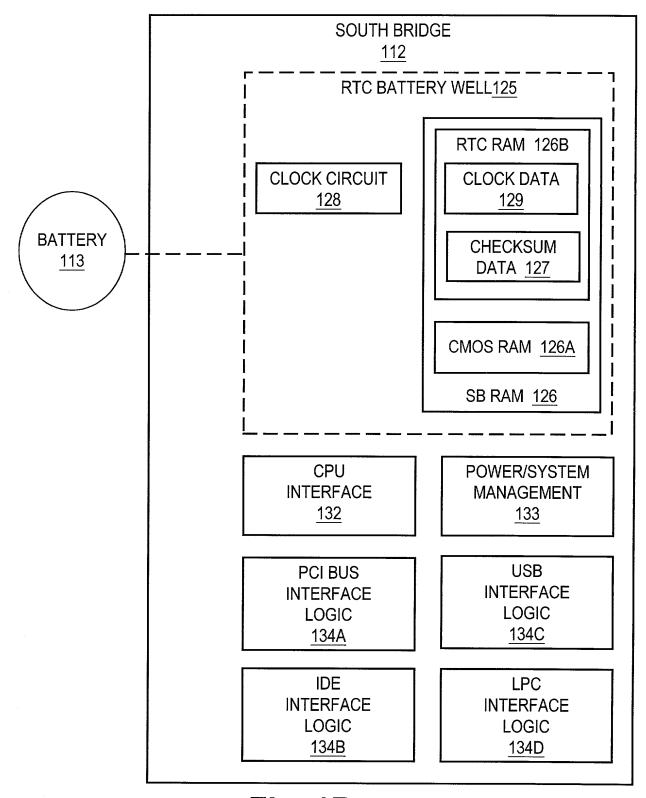


Fig. 1B (Prior Art)

POWER SUPPLY INITIALIZATION POWER SUPPLY GENERATES A POWER GOOD SIGNAL TO THE NORTH BRIDGE 136

UP RECEIVING THE POWER GOOD SIGNAL, THE SOUTH BRIDGE STOPS ASSERTING THE RESET SIGNAL FOR THE PROCESSOR 138

THE PROCESSOR READS THE DEFAULT JUMP LOCATION, USUALLY AT FFFF0h 140

THE PROCESSOR JUMPS TO THE BIOS CODE LOCATION IN THE ROM BIOS, COPIES THE BIOS CODE TO RAM, AND BEGINS PROCESSING BIOS CODE INSTRUCTIONS FROM RAM 142

BIOS CODE PERFORMS POWER ON SELF TEST (POST) 144

BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 146

BIOS CODE PERFORMS ADDITIONAL SYSTEM TESTS, SUCH AS THE RAM COUNT-UP TEST, AND SYSTEM INVENTORY, SUCH AS IDENTIFYING COM AND LPT PORTS 148

BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 150

BIOS CODE IDENTIFIES THE BOOT LOCATION 152

BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 154

Fig. 2A (Prior Art)

**/** 170

# INTERRUPT CONTROLLER RECEIVES A REQUEST FOR SYSTEM MANAGEMENT MODE (SMM) 172

INTERRUPT CONTROLLER SIGNALS THE REQUEST FOR SMM TO THE PROCESSOR BY ASSERTING THE SYSTEM MANAGEMENT INTERRUPT (SMI#) SIGNAL 174

PROCESSOR RECOGNIZES THE REQUEST FOR SMM AND ASSERTS THE SMI ACTIVE (SMIACT#) SIGNAL 176

SYSTEM RECOGINIZES THE SMIACT# SIGNAL, DISABLES ACCESS TO RAM, AND ENABLES ACCESS TO SYSTEM MANAGEMENT RAM (SMRAM) SPACE 178

CURRENT PROCESSOR STATE IS SAVED TO SMRAM 180

PROCESSOR RESETS TO SMM DEFAULT STATE AND ENTERS SMM 182

PROCESSOR READS DEFAULT POINTER AND JUMPS INTO SMRAM SPACE 184

STATUS REGISTERS ARE CHECKED TO IDENTIFY THE SMI REQUEST 186

SMI HANDLER SERVICES THE SMI REQUEST 188

SMI HANDLER ISSUES RETURN FROM SMM (RSM) INSTRUCTION TO PROCESSOR 190

PROCESSOR RESTORES SAVED STATE INFORMATION AND CONTINUES

NORMAL OPERATION 192

Fig. 2B (Prior Art)

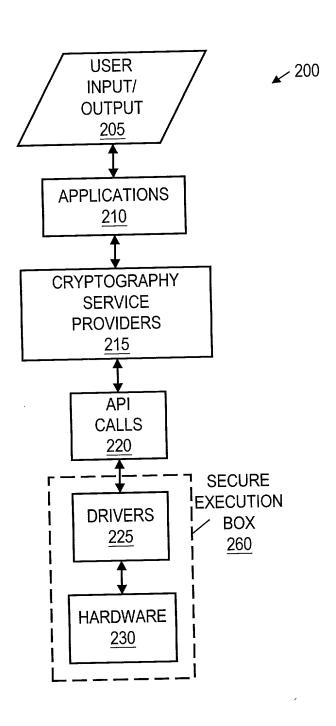
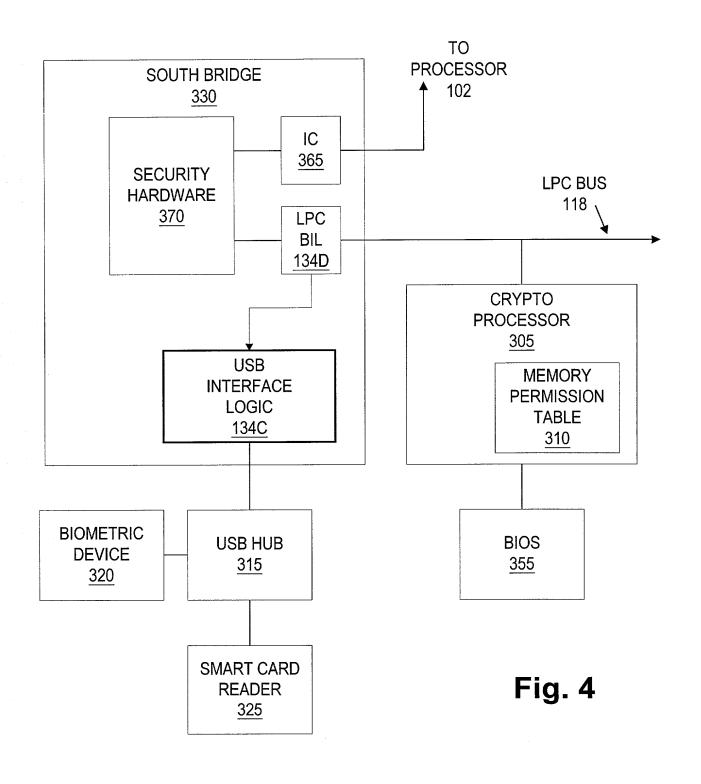


Fig. 3



the trail that the state that the first that

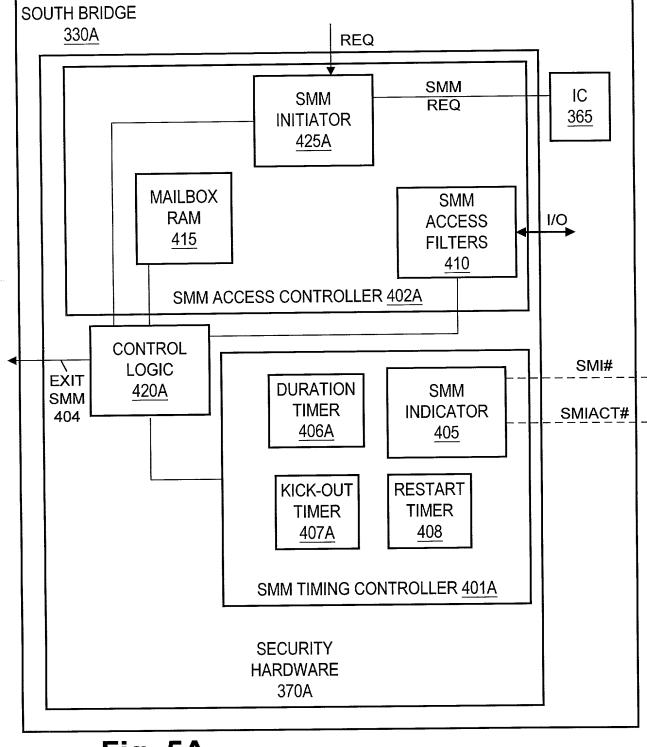


Fig. 5A

8 / 73

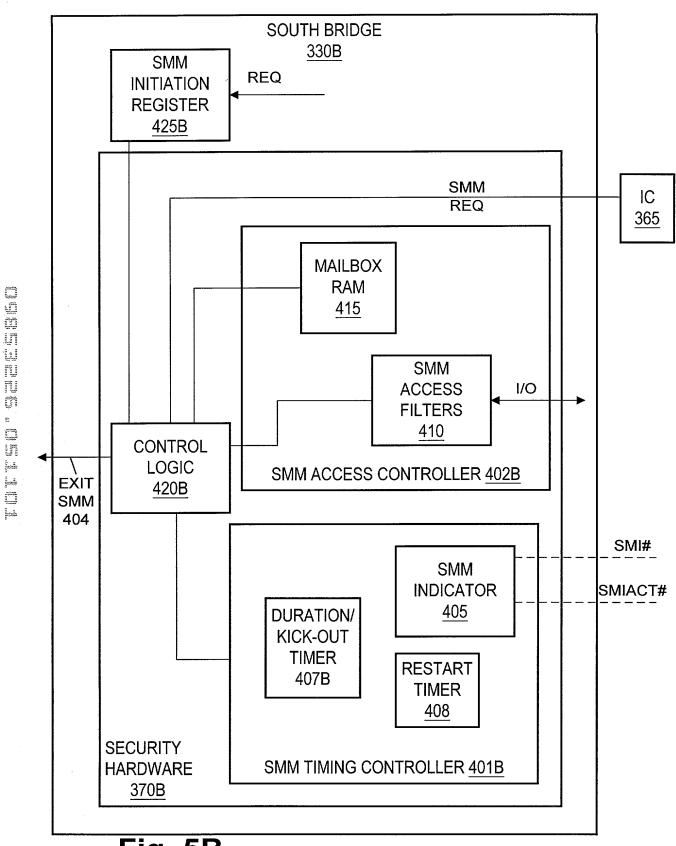


Fig. 5B

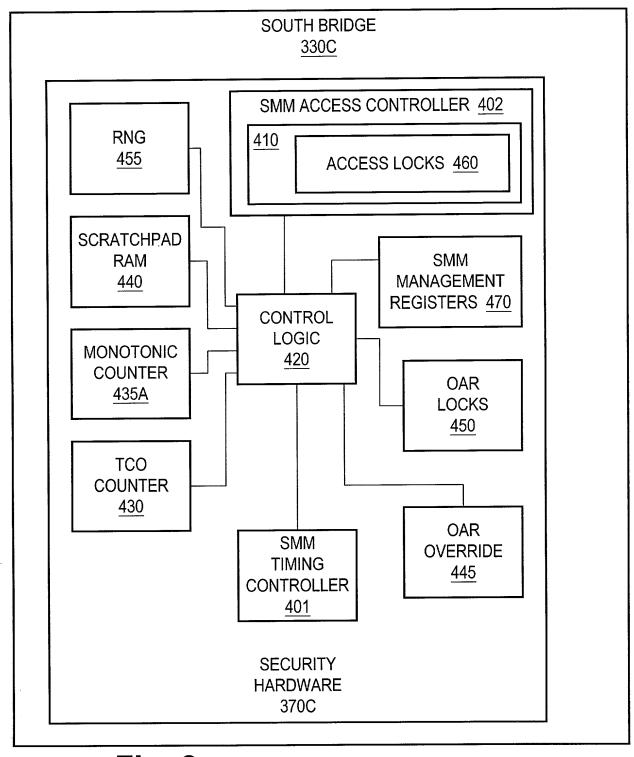
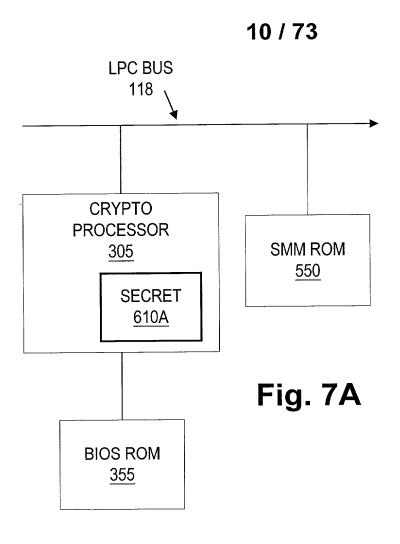


Fig. 6



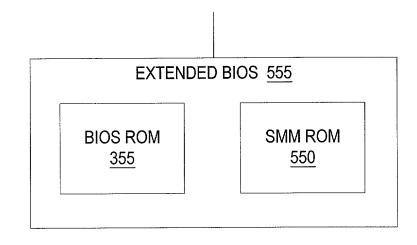


Fig. 7B

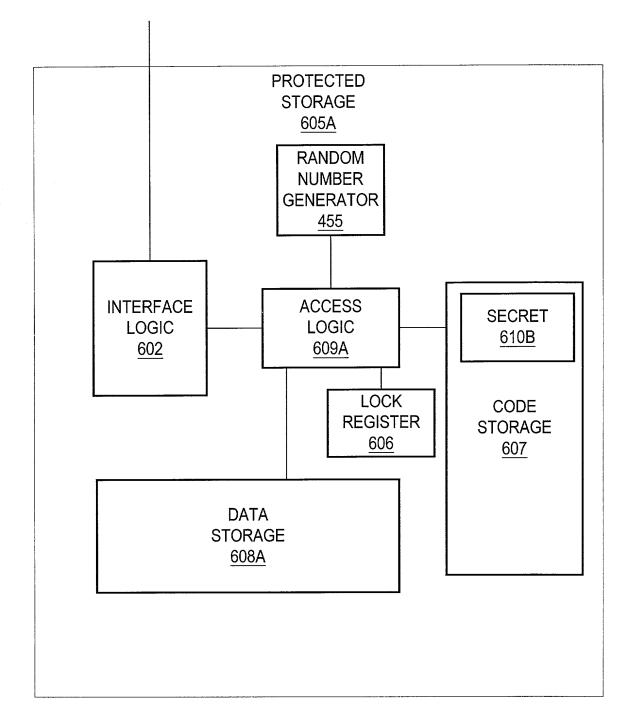


Fig. 7C

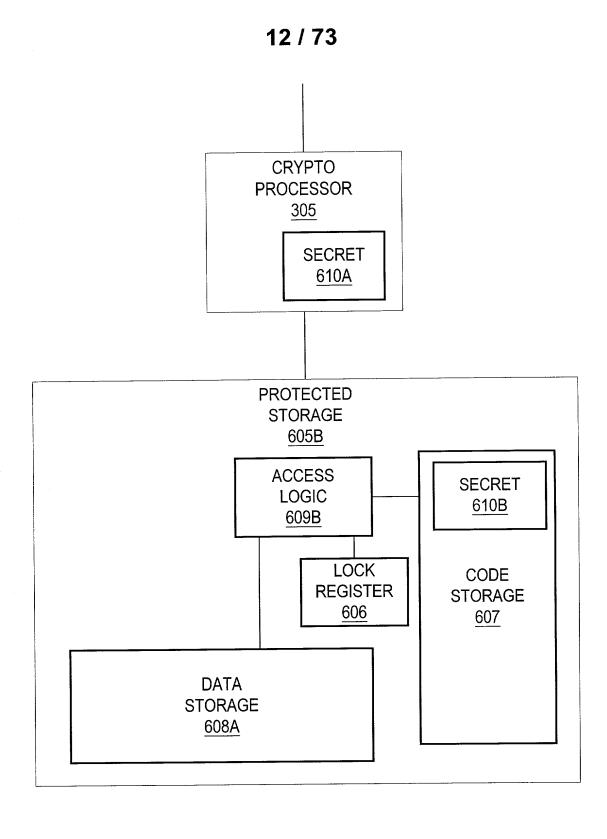


Fig. 7D

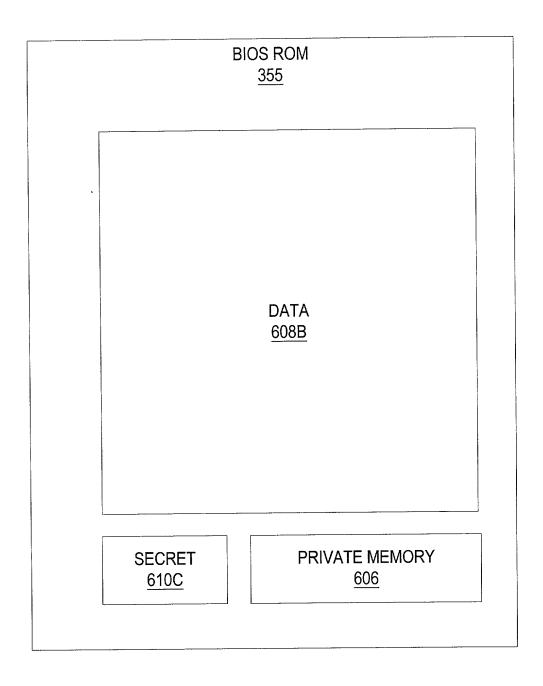


Fig. 8A

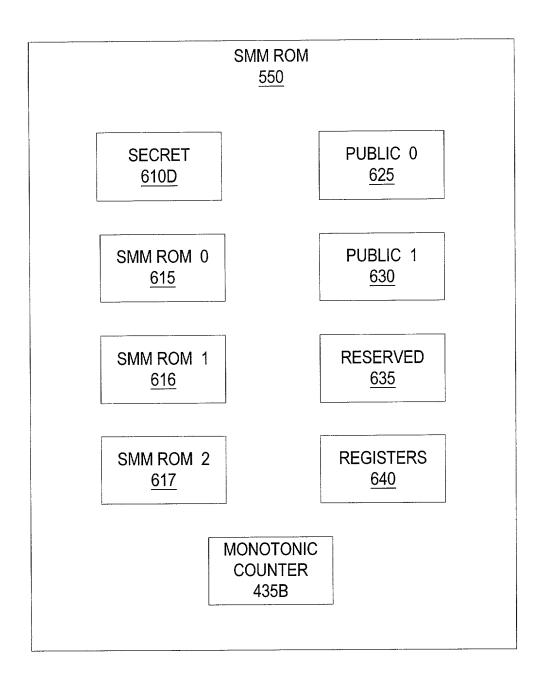


Fig. 8B

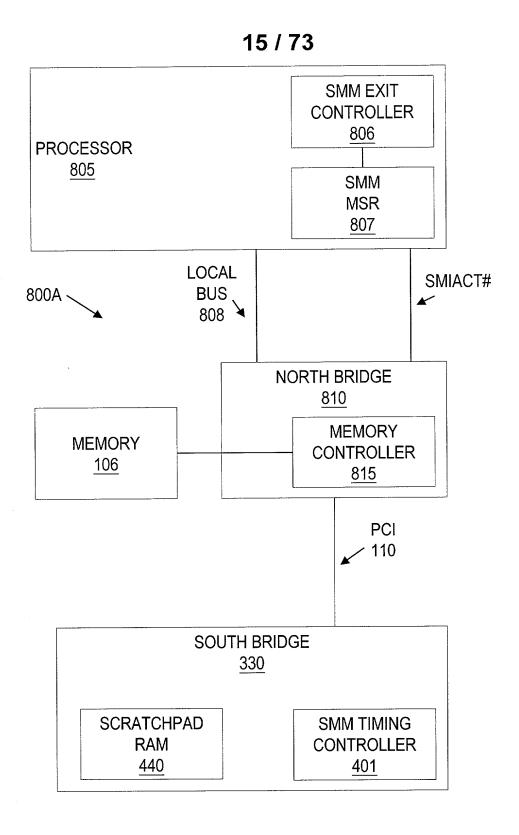


Fig. 9A

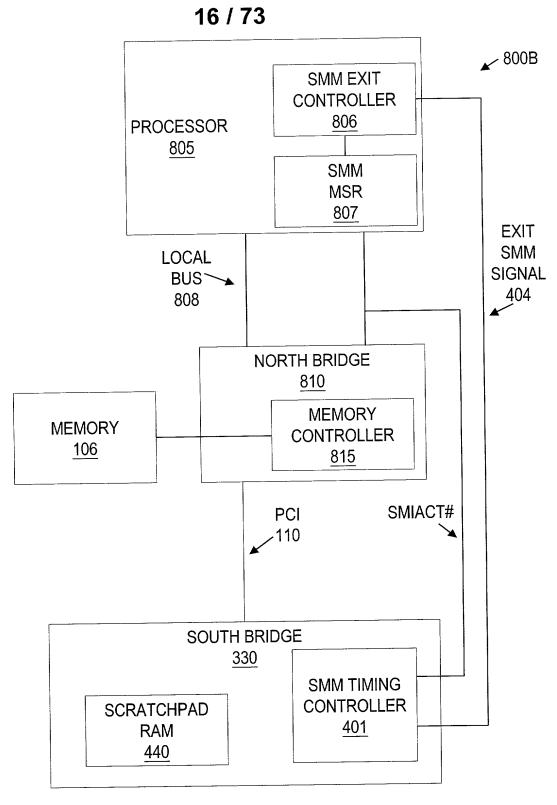
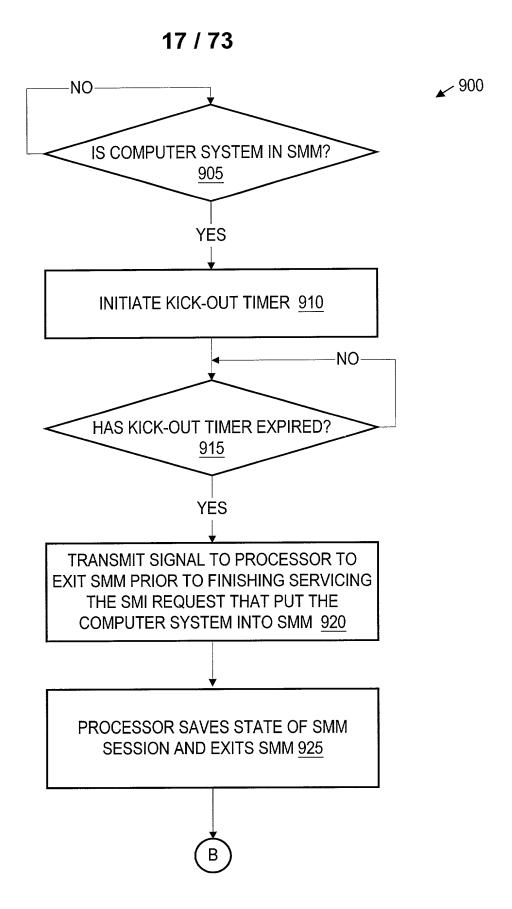


Fig. 9B



**Fig. 10A** 

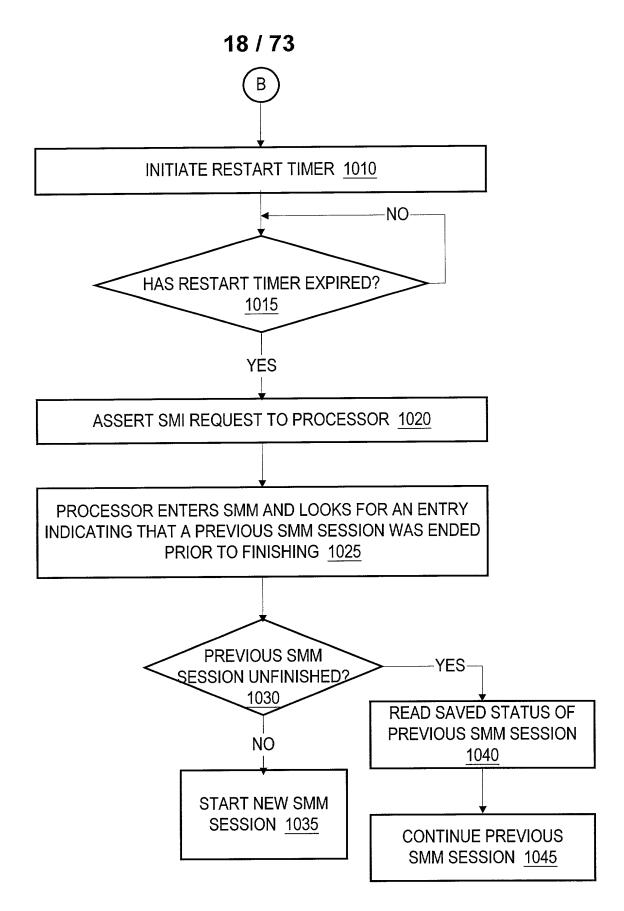
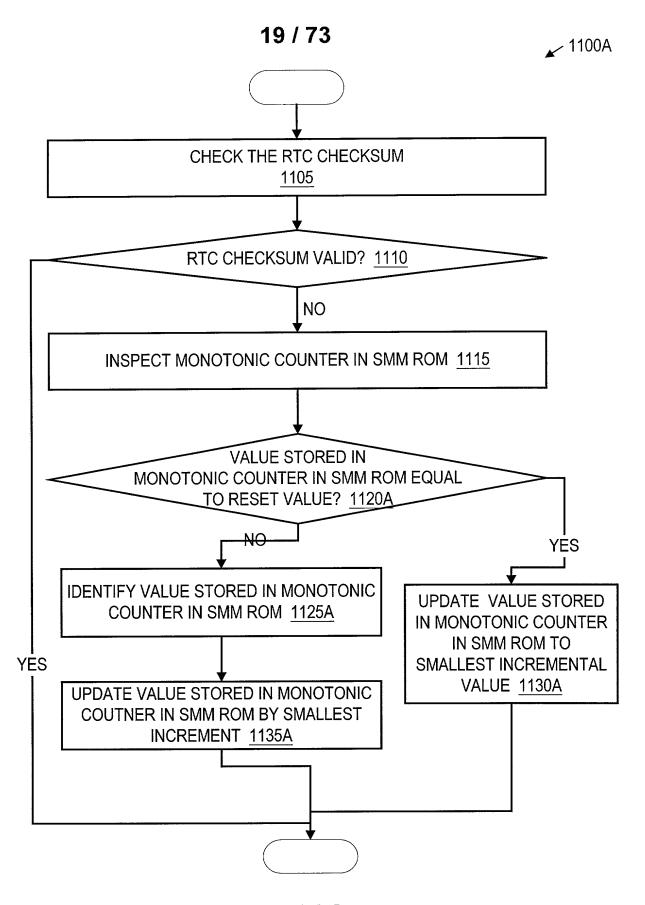


Fig. 10B



**Fig. 11A** 

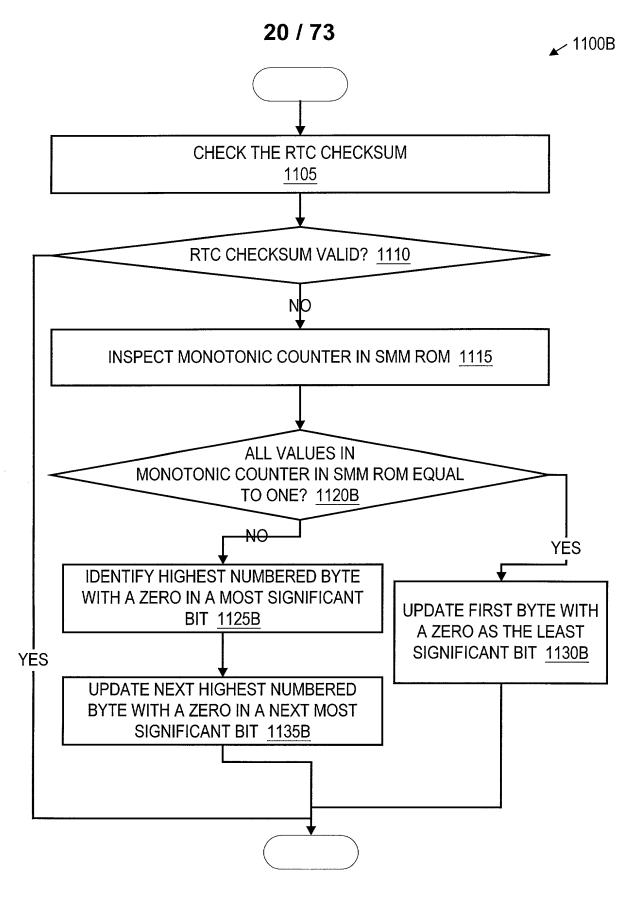
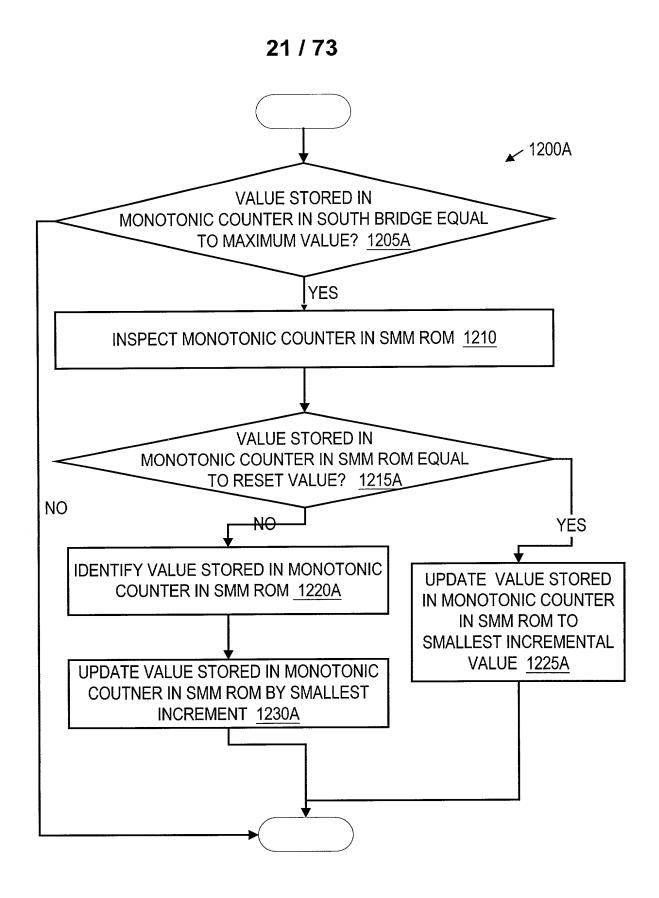
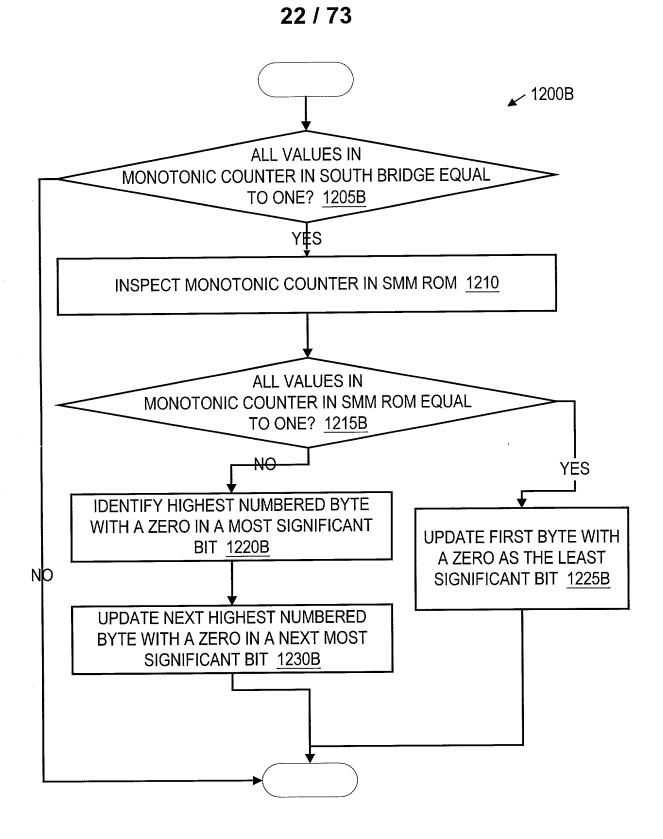


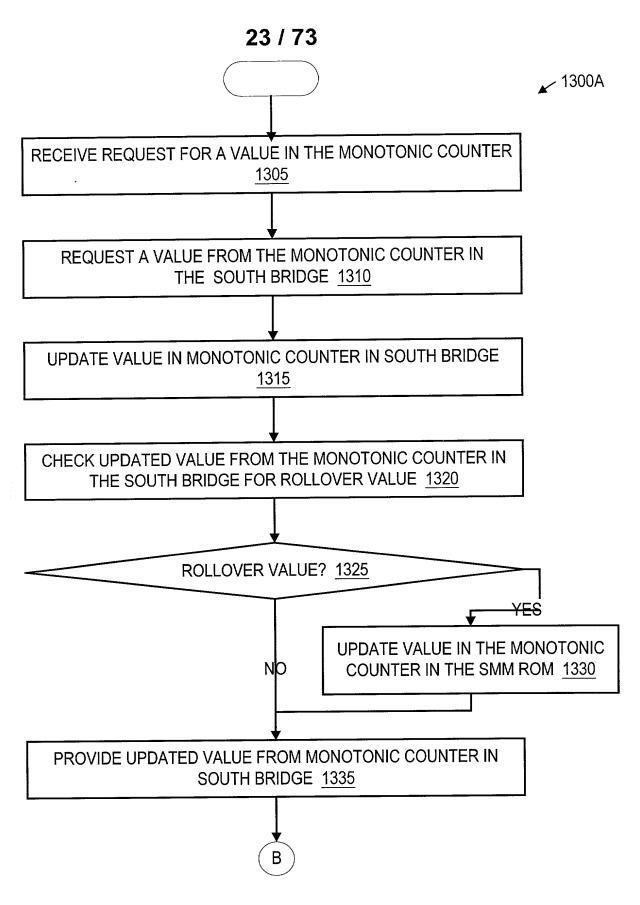
Fig. 11B



**Fig. 12A** 



**Fig. 12B** 



**Fig. 13A** 

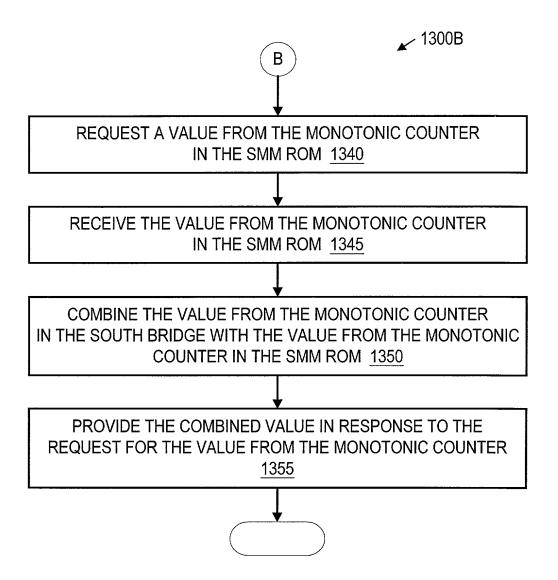
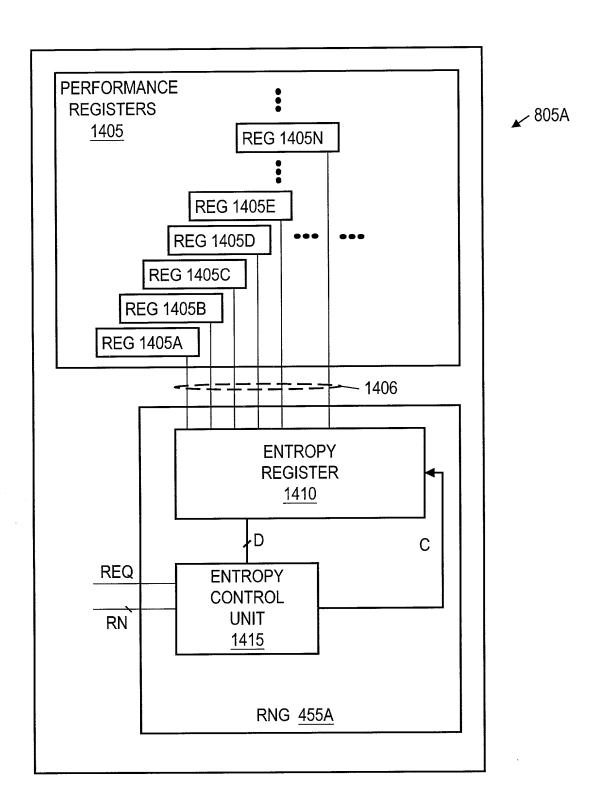


Fig. 13B



**Fig. 14A** 

26 / 73

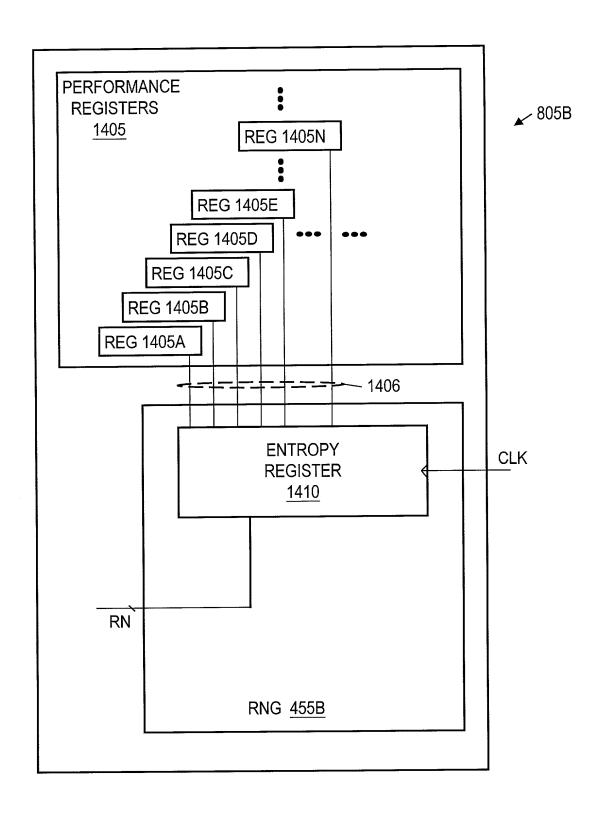


Fig. 14B

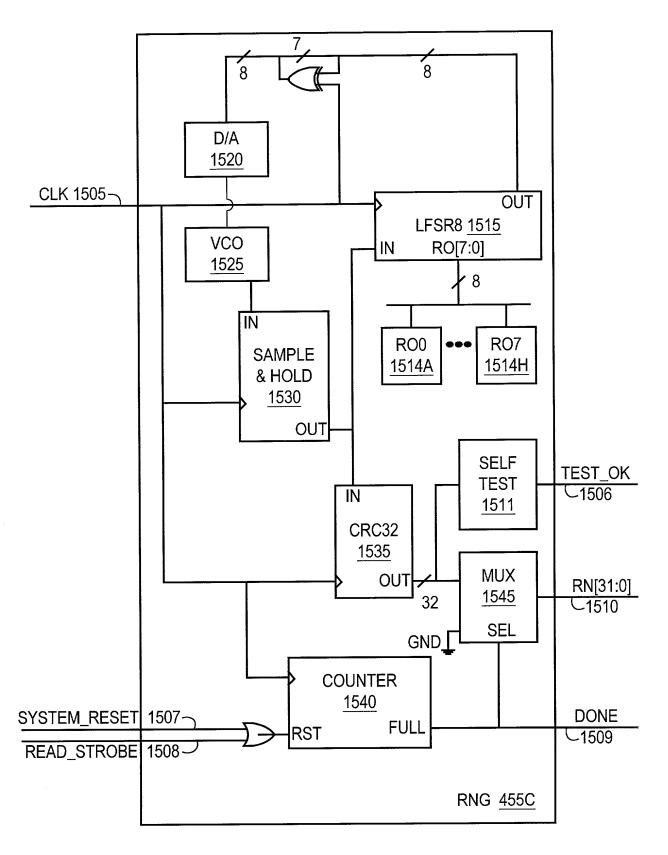
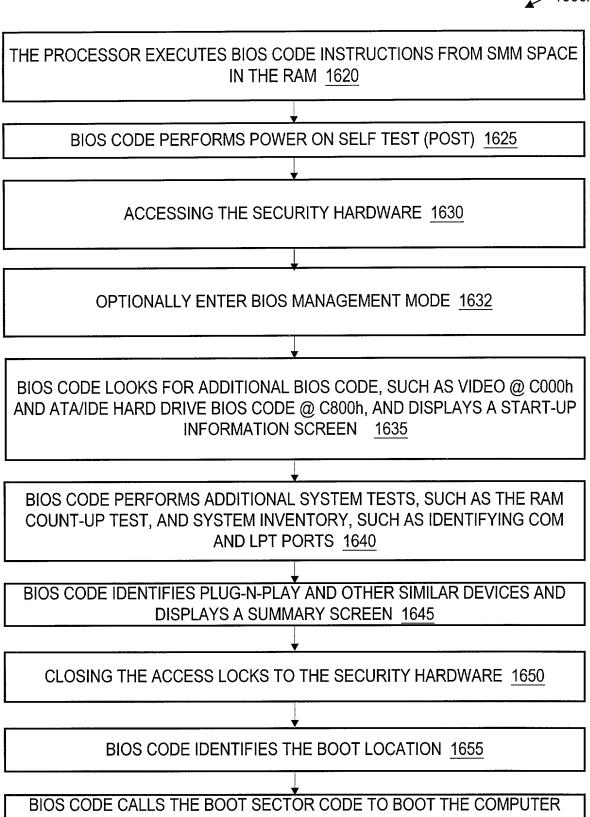


Fig. 15



**Fig. 16A** 

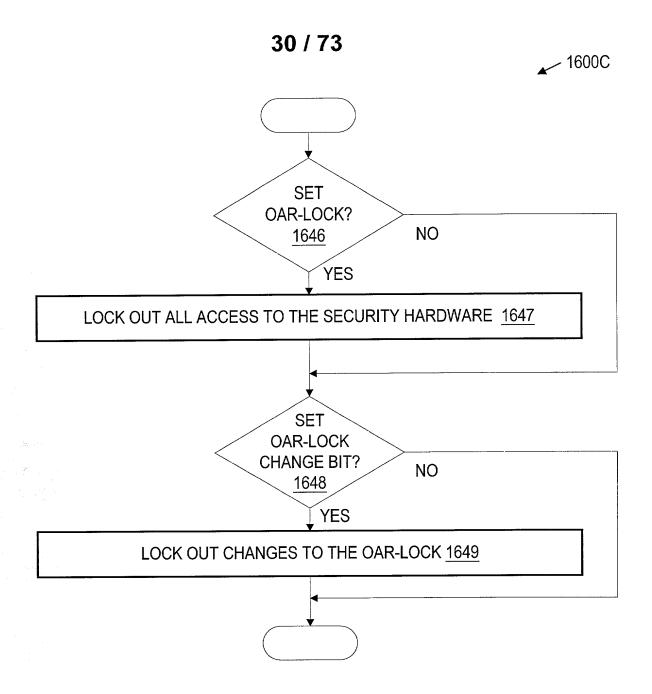
SYSTEM 1660

\_\_\_ 1600B

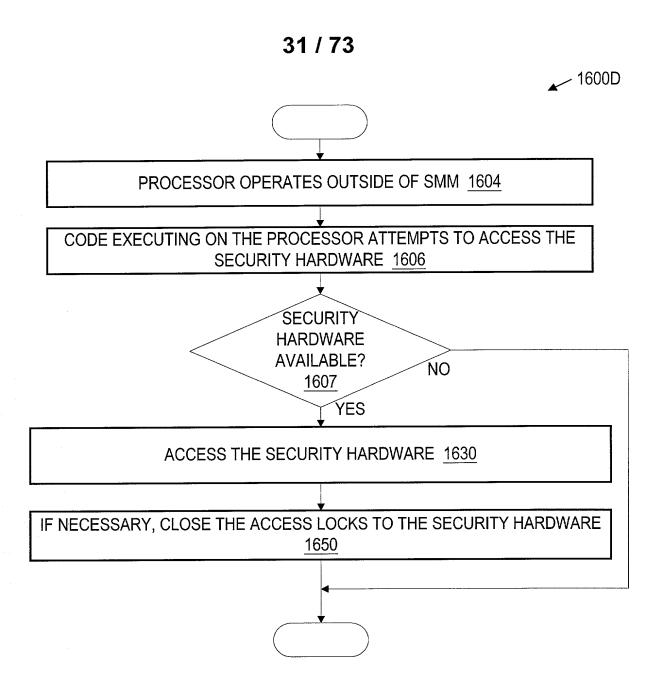
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615 THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620 ACCESSING THE SECURITY HARDWARE 1630 OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632 BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635 BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645 CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650 BIOS CODE IDENTIFIES THE BOOT LOCATION 1655 BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

**Fig. 16B** 

don't that the trade and trade them them that



**Fig. 16C** 



**Fig. 16D** 

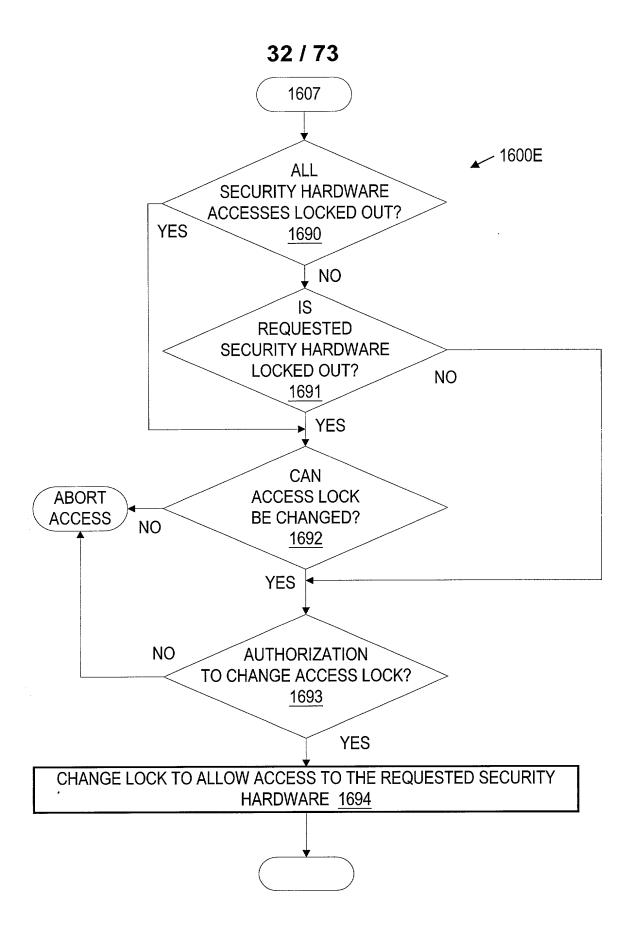


Fig. 16E

THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM 1605

OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615

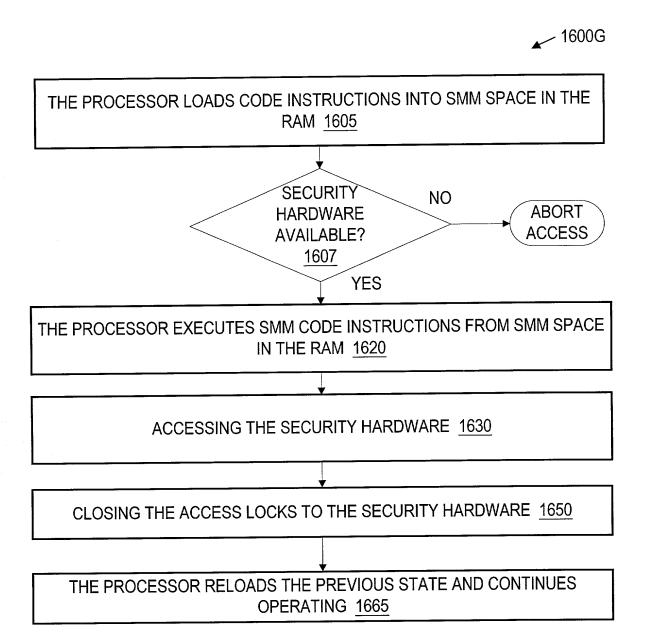
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620

ACCESSING THE SECURITY HARDWARE 1630

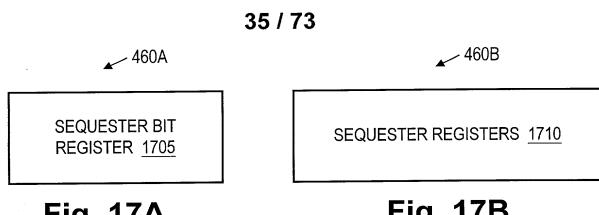
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650

THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING 1665

**Fig. 16F** 

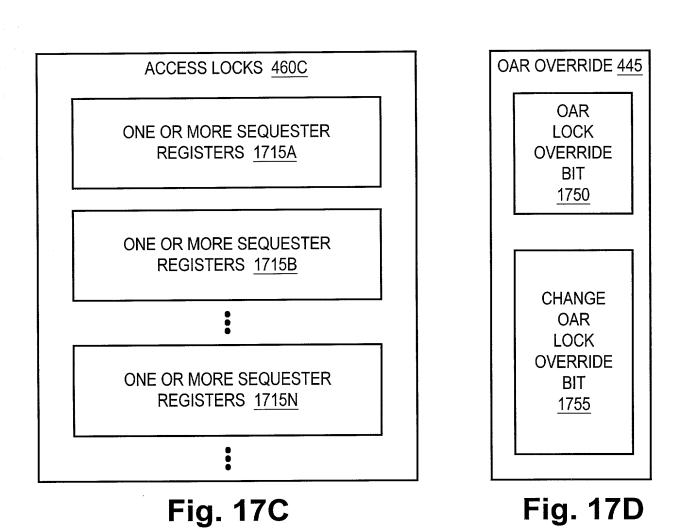


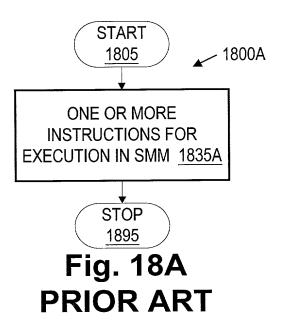
**Fig. 16G** 



**Fig. 17A** 

Fig. 17B





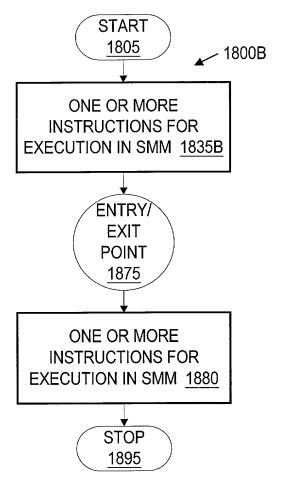
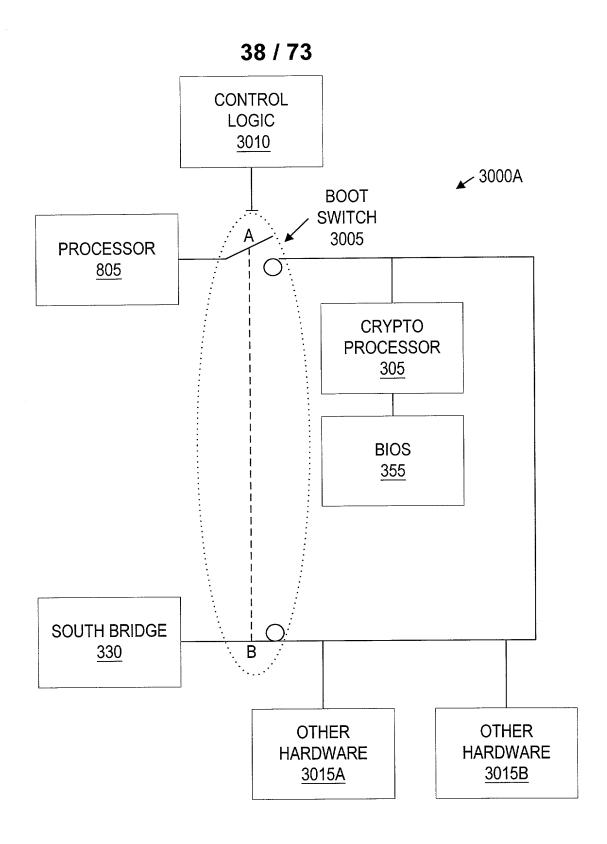


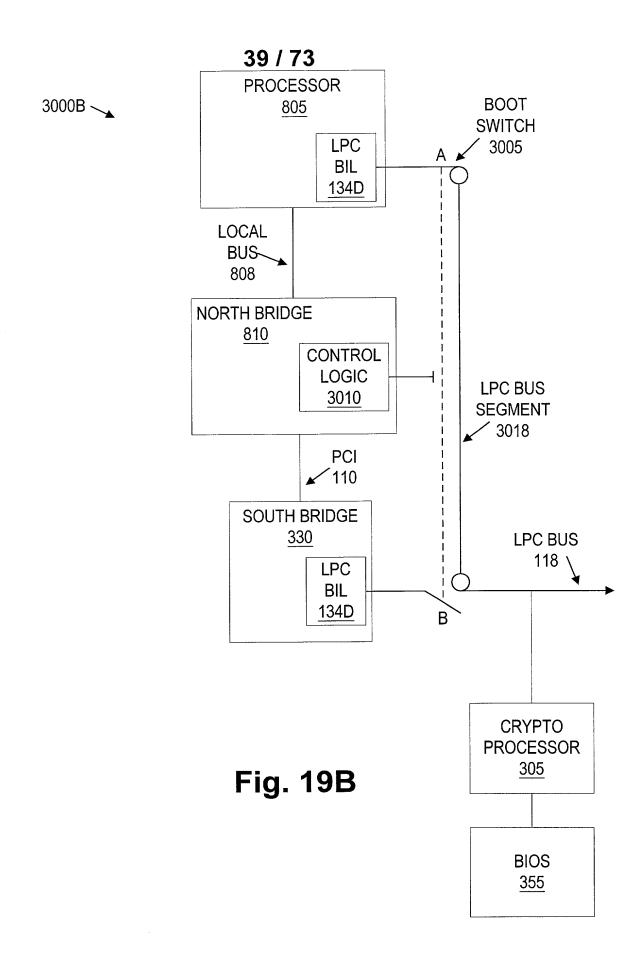
Fig. 18B

The first first first only first first first first

Fig. 18C



**Fig. 19A** 



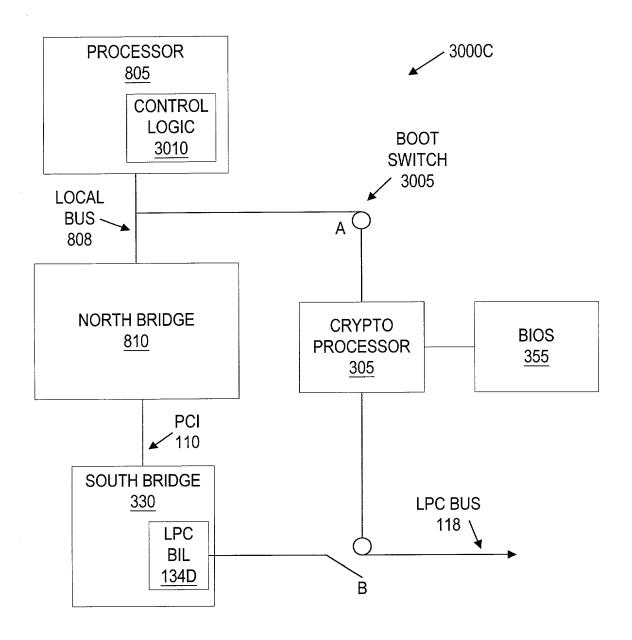


Fig. 19C

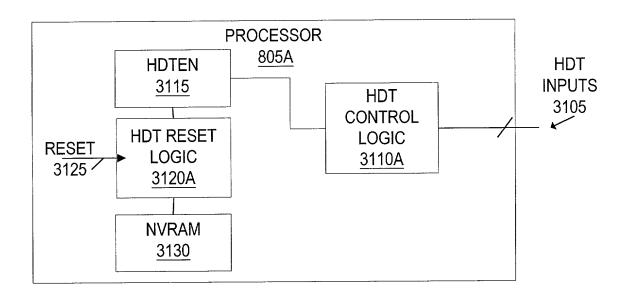
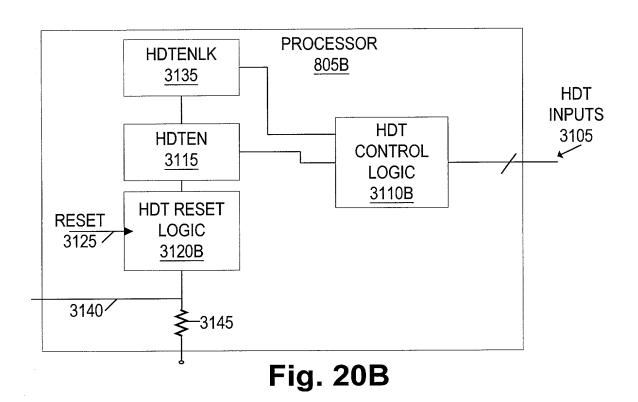
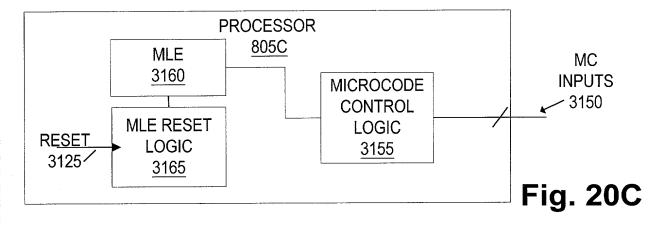
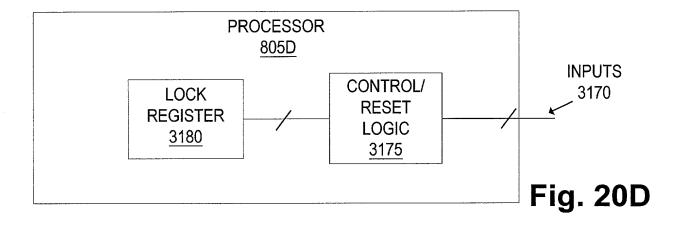


Fig. 20A







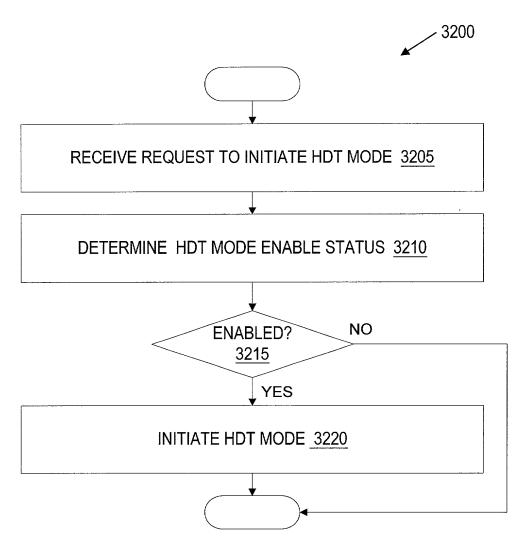


Fig. 21

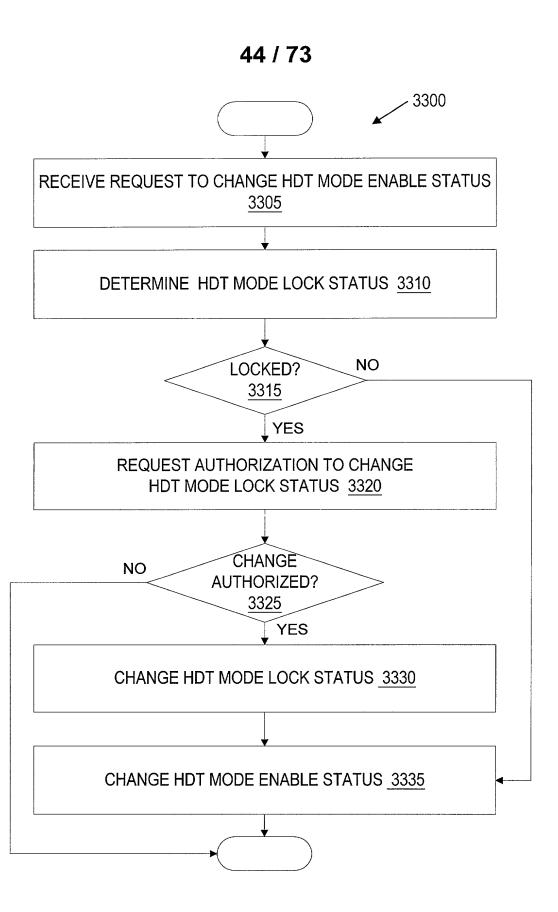


Fig. 22

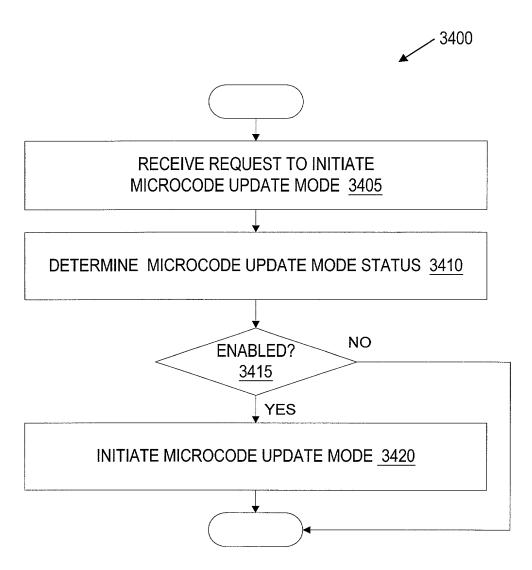


Fig. 23

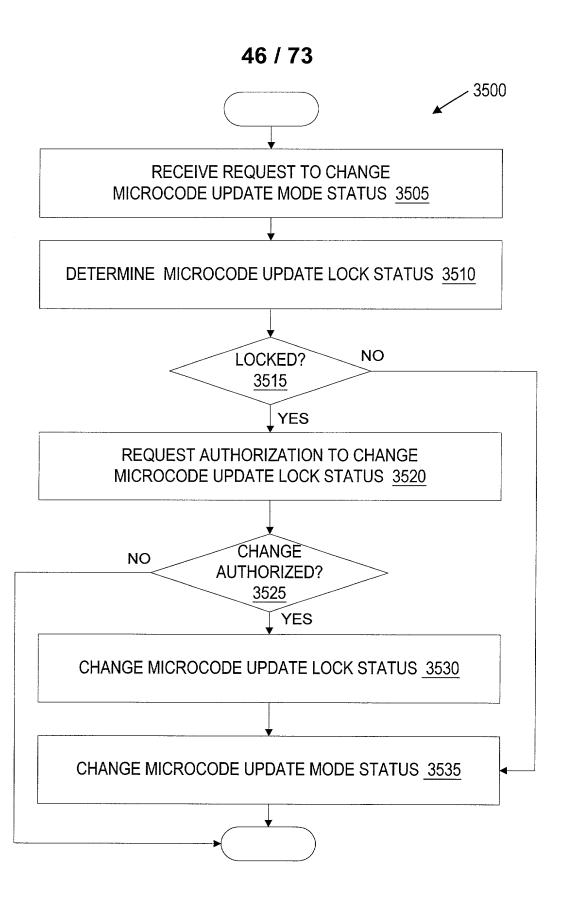


Fig. 24

∠ 3600A A SECURITY DEVICE RECEIVES A TRANSACTION REQUEST FOR A STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3605A THE SECURITY DEVICE PROVIDES ACCESS CONTROL FOR THE STORAGE DEVICE 3610A THE SECURITY DEVICE MAPS THE STORAGE LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE STORAGE DEVICE 3615A THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3620A THE STORAGE DEVICE PERFORMS THE REQUESTED TRANSACTION 3625A

**Fig. 25A** 

3600B A CRYPTO-PROCESSOR RECEIVES A TRANSACTION REQUEST FOR A MEMORY LOCATION ASSOCIATED WITH A MEMORY CONNECTED TO THE CRYPTO-PROCESSOR 3605B THE CRYPTO-PROCESSOR PROVIDES ACCESS CONTROL FOR THE MEMORY 3610B THE CRYPTO-PROCESSOR MAPS THE MEMORY LOCATION IN THE TRANSACTION REQUEST ACCORDING TO THE ADDRESS MAPPING OF THE MEMORY 3615B THE CRYPTO-PROCESSOR PROVIDES THE TRANSACTION REQUEST TO THE MEMORY 3620B THE MEMORY PERFORMS THE REQUESTED TRANSACTION 3625B

Fig. 25B

\_\_ 3610A

THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705 NO LOCKED? 3710 YES THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715 THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720 THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725 NO **CORRECT?** 3730 **END** YES THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

Fig. 26

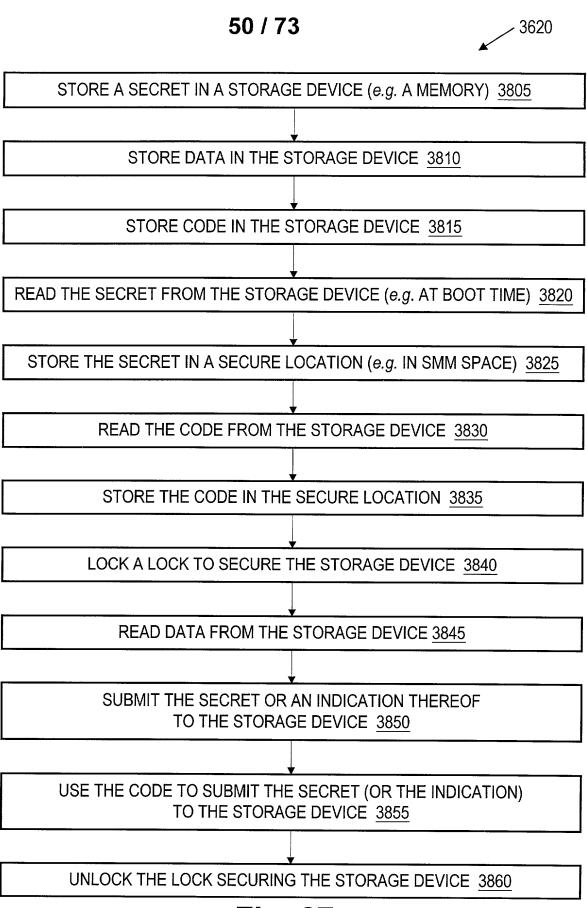


Fig. 27

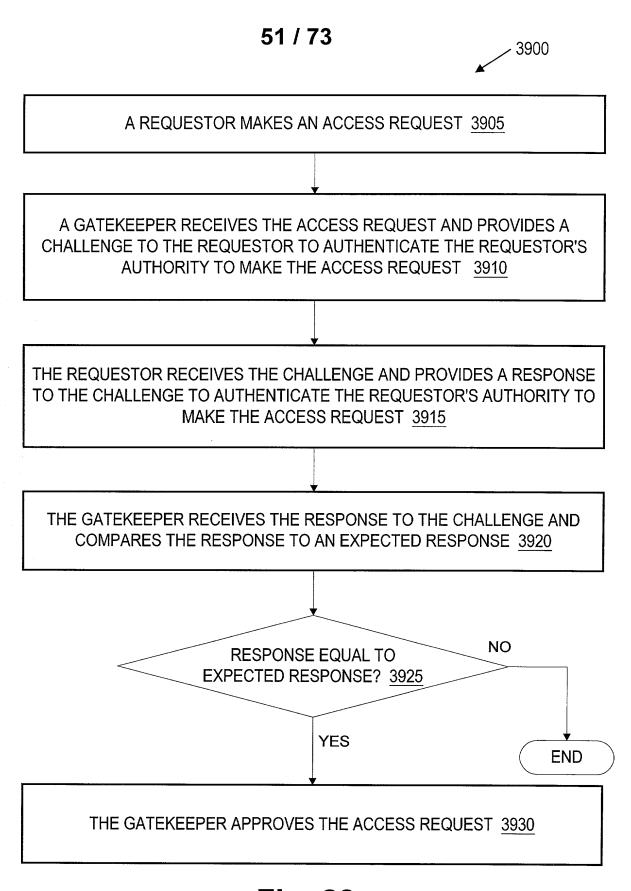


Fig. 28 (Prior Art)

half the train and may may sing from the train 

53 / 73

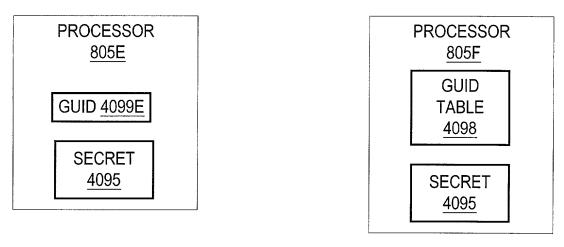
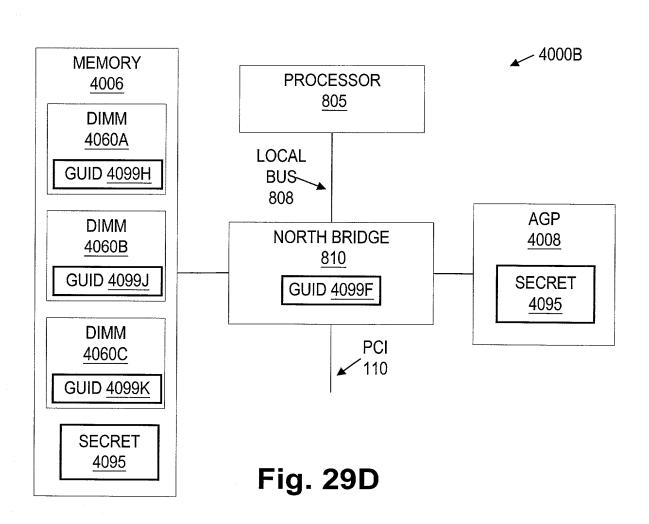
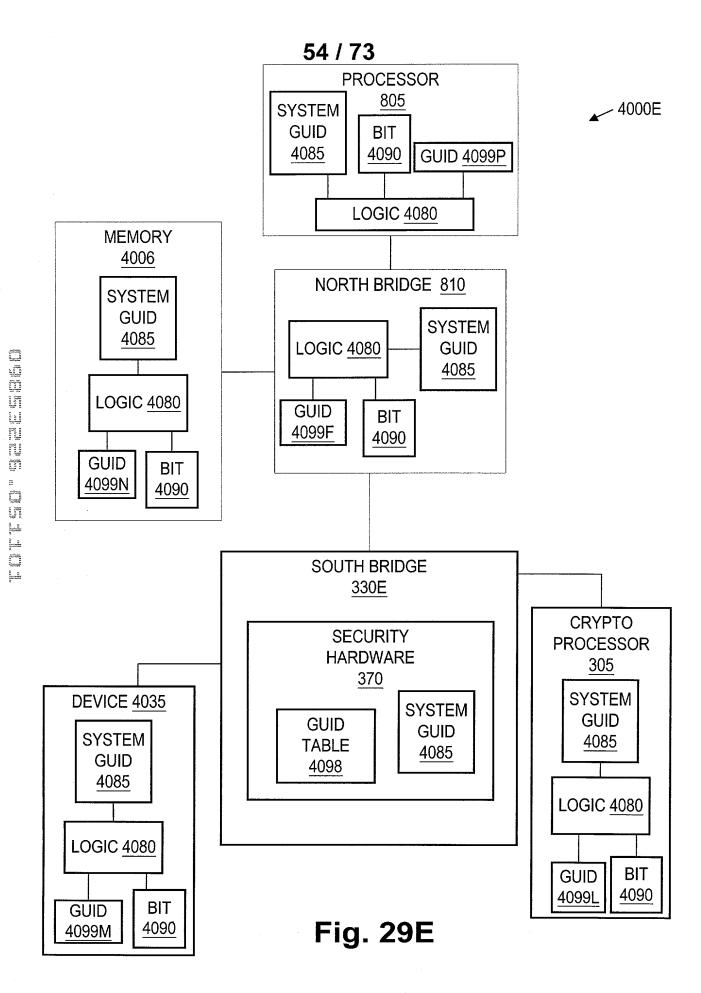


Fig. 29B

Fig. 29C





4100A

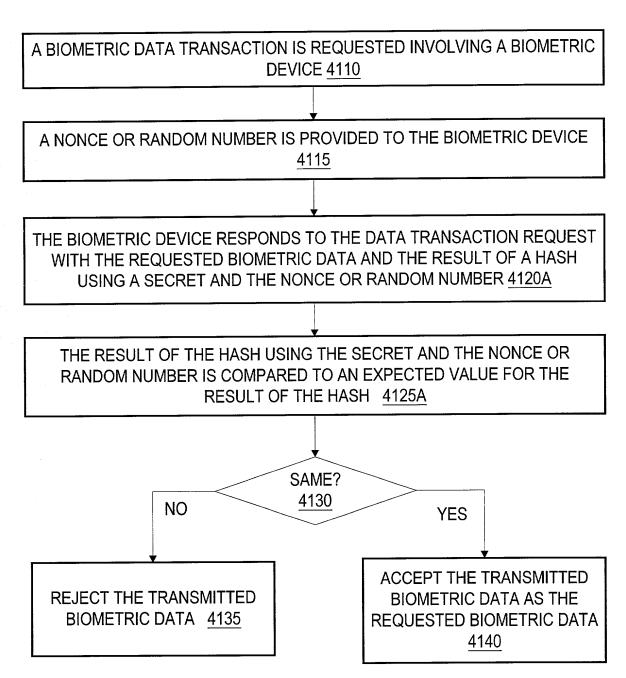


Fig. 30A

4100B

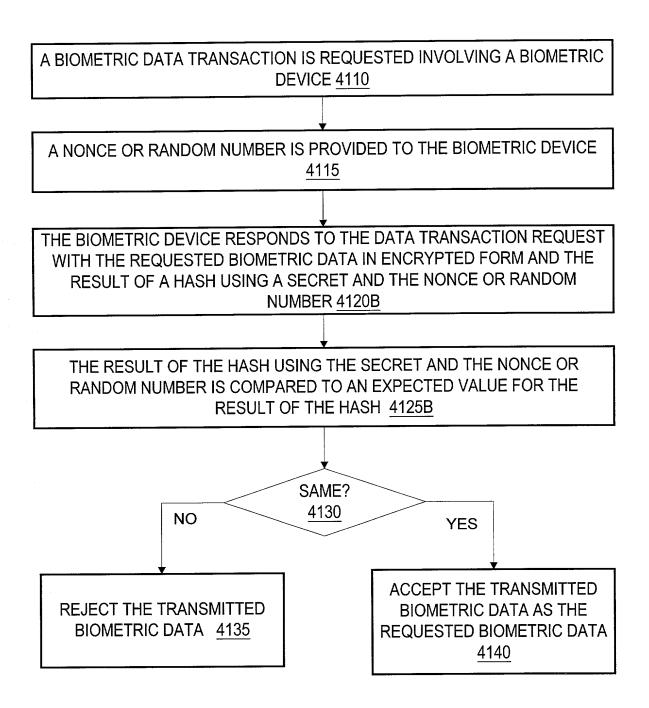
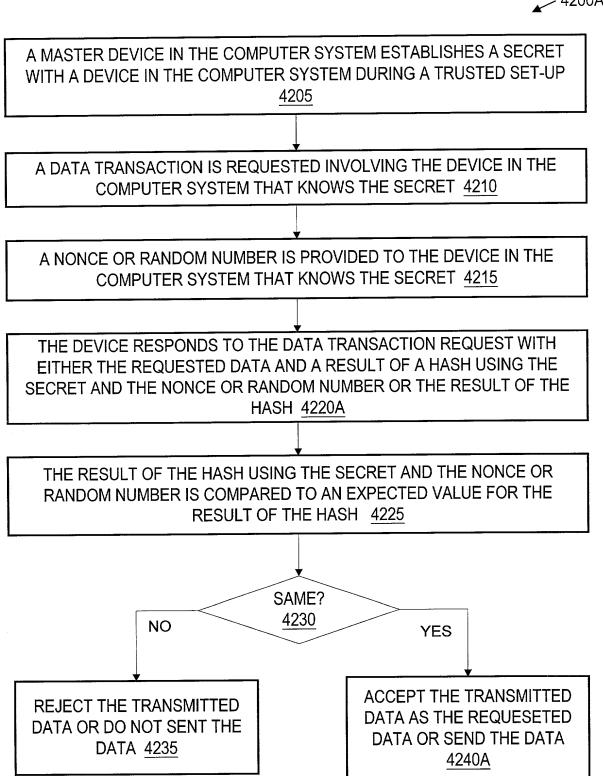
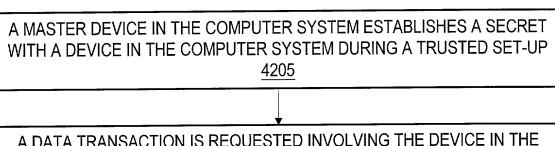


Fig. 30B



**Fig. 31A** 

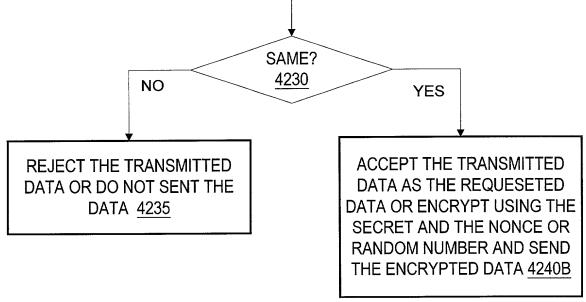


A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY EITHER ENCRYPTING THE REQUESTED DATA USING THE SECRET AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4220B

THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225



**Fig. 31B** 



A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305 A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310 A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315 THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4320A THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325 SAME? 4330 NO YES ACCEPT THE TRANSMITTED REJECT THE TRANSMITTED DATA AS THE REQUESETED DATA OR DO NOT SENT THE DATA OR SEND THE DATA **DATA 4335** 4340A

**Fig. 32A** 

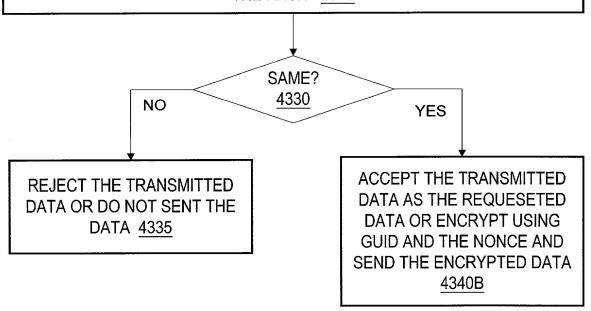
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305

A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310

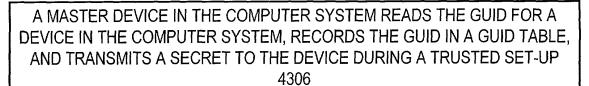
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE GUID AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320B

THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325



**Fig. 32B** 

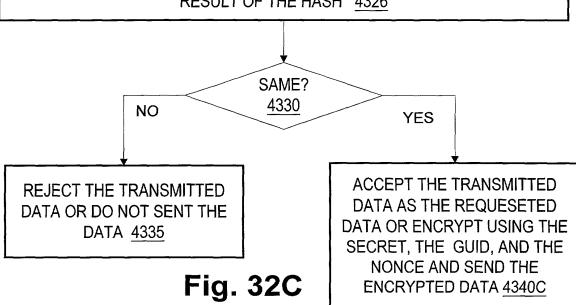


A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4311

A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID THAT KNOWS THE SECRET 4316

THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320C

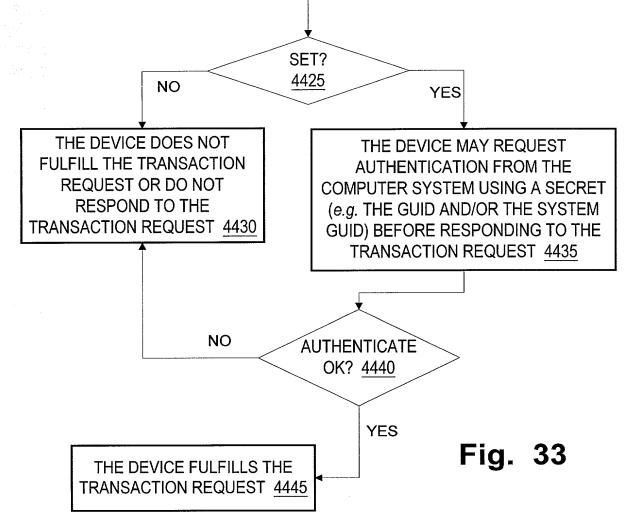
THE RESULT OF THE HASH USING THE SECRET, THE GUID, AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4326



4400 A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4405 THE DEVICE MAY RECEIVE A SYSTEM GUID FROM THE MASTER DEVICE AND STORE THE SYSTEM GUID 4410

THE DEVICE SETS A INTRODUCED BIT IN RESPONSE TO JOINING THE **COMPUTER SYSTEM 4415** 

THE DEVICE RECEIVES A TRANSACTION REQUEST FROM THE COMPUTER SYSTEM AND THE DEVICE CHECKS IF ITS INTRODUCED BIT IS SET 4420



4500

THE DEVICE OR THE MASTER DEVICE INITIATES A REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4505

THE DEVICE AND THE MASTER DEVICE AUTHENTICATE EACH OTHER USING THE GUID AND/OR THE SYSTEM GUID IN RESPONSE TO THE REQUEST FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4510

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE AND THE MASTER DEVICE SUCCESSFULLY AUTHENTICATING EACH OTHER 4515

Fig. 34

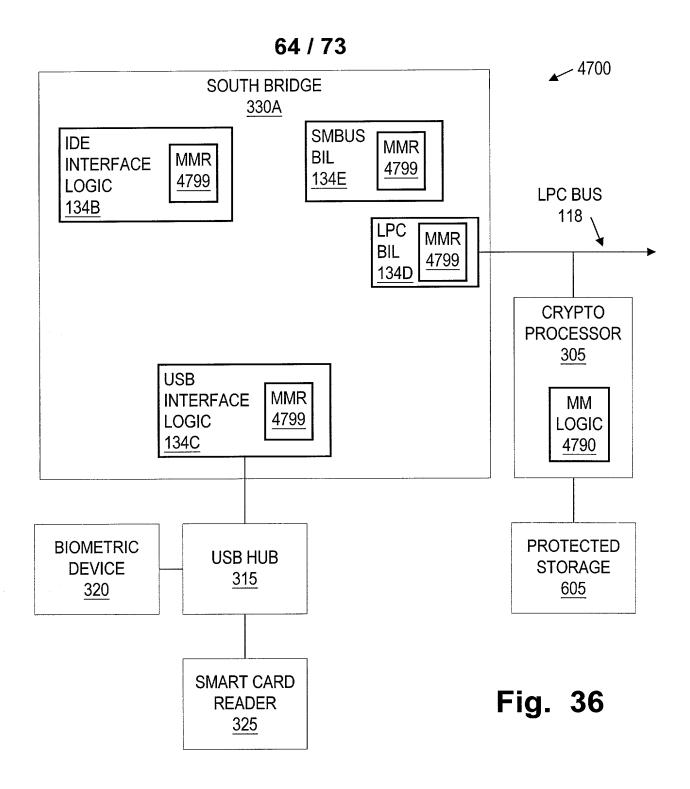
4600

THE DEVICE RECEIVING A COMMAND FOR THE DEVICE TO LEAVE THE COMPUTER SYSTEM 4605

THE DEVICE RECEIVING A MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4610

THE DEVICE RESETS THE INTRODUCED BIT IN RESPONSE TO THE DEVICE RECEIVING THE MAINTENANCE KEY THAT SUCCESSFULLY AUTHENTICATES 4615

Fig. 35



4800

TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER  $\frac{4805}{}$ 

SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810

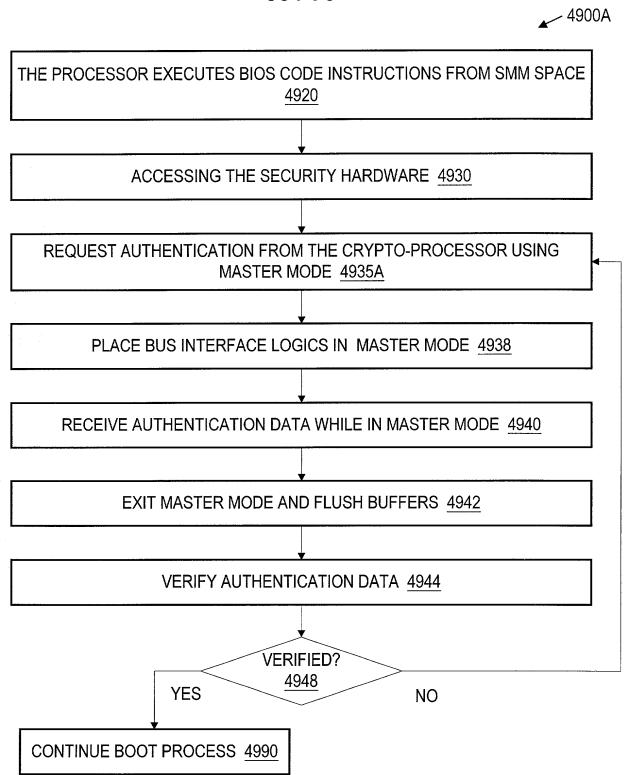
THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815

THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820

THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE MASER MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4825

Fig. 37





**Fig. 38A** 

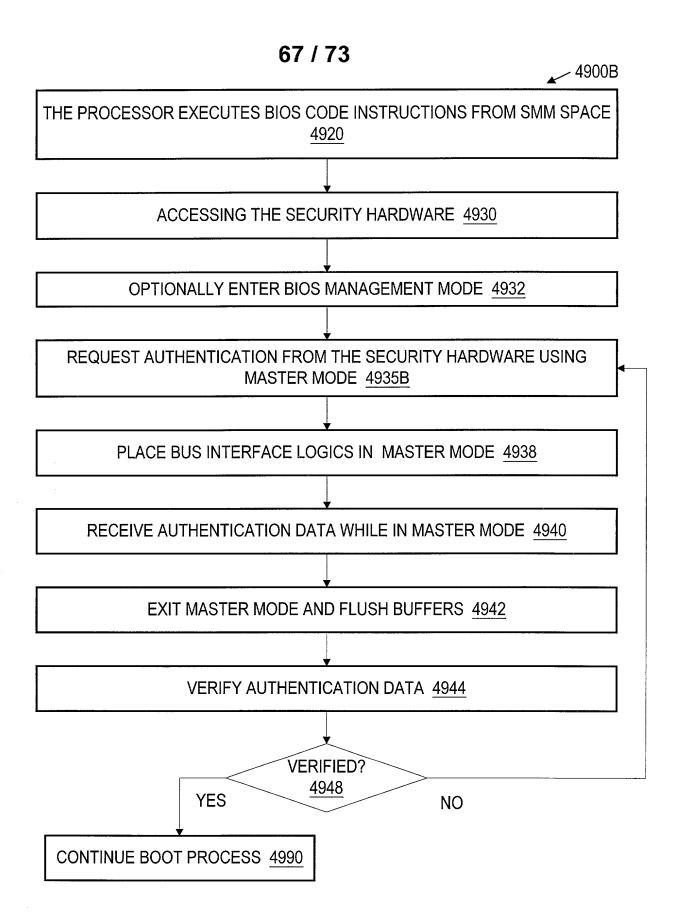
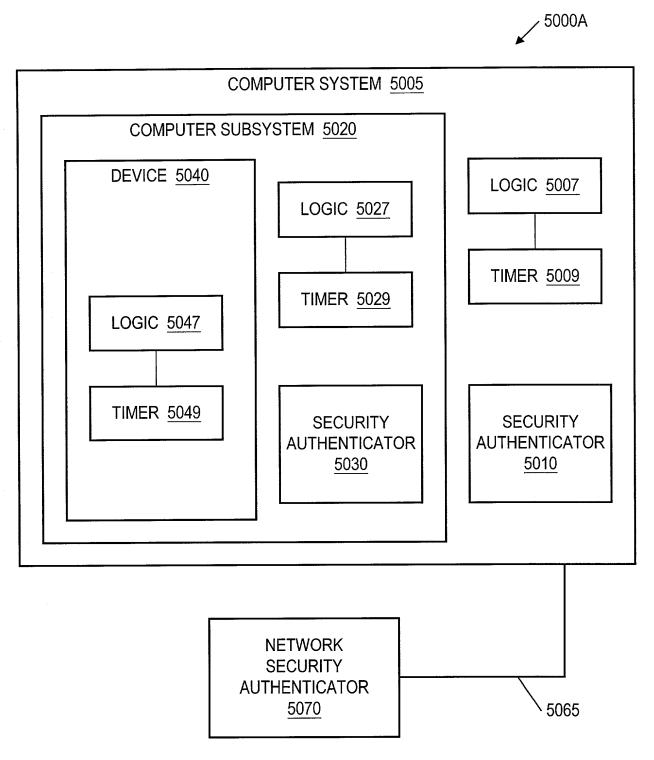
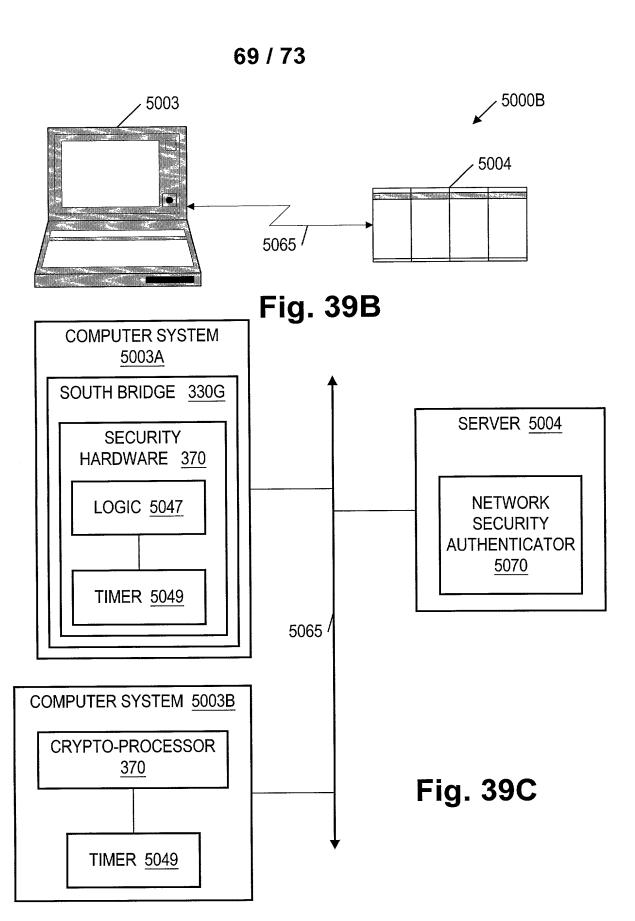


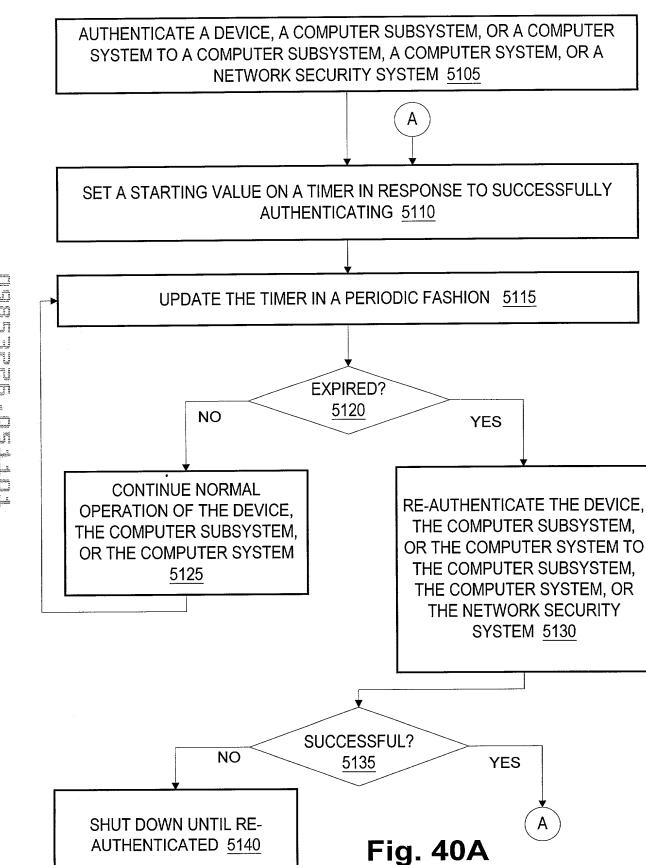
Fig. 38B

68 / 73

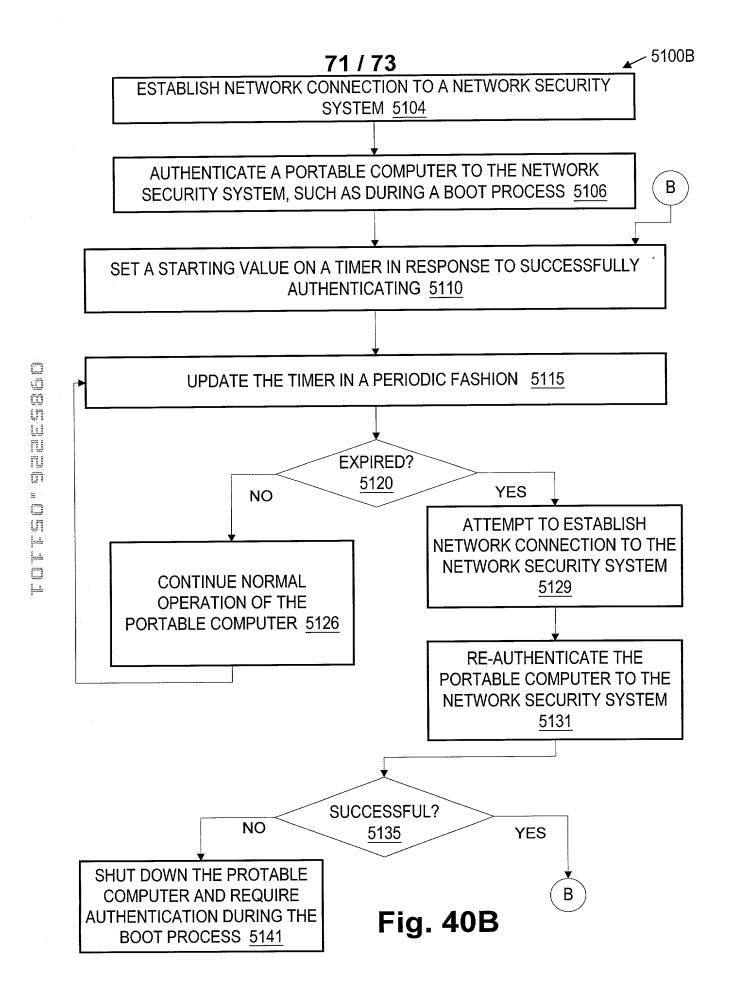


**Fig. 39A** 





The light from the light from the thing the th m 



72 / 73

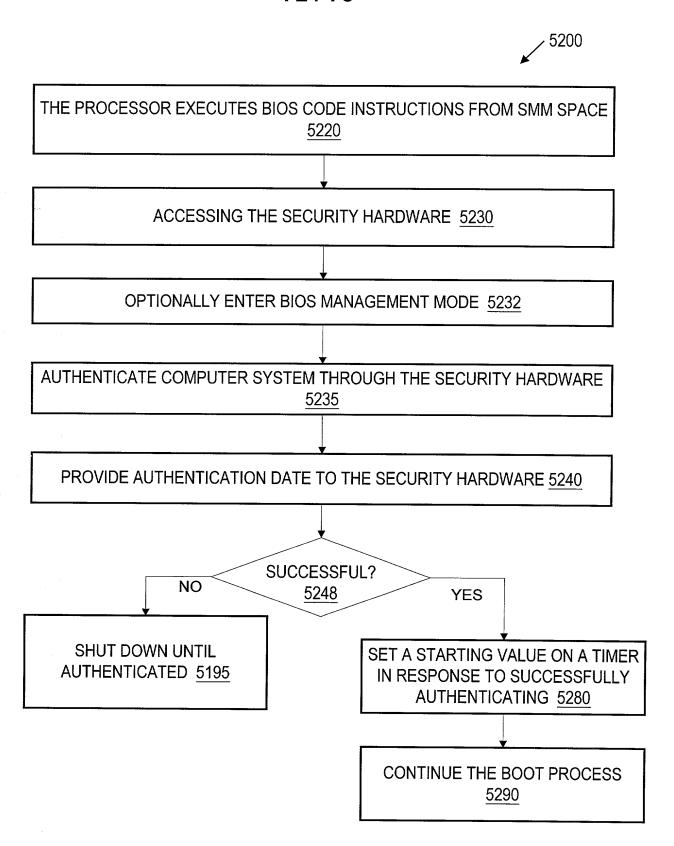


Fig. 41

73 / 73

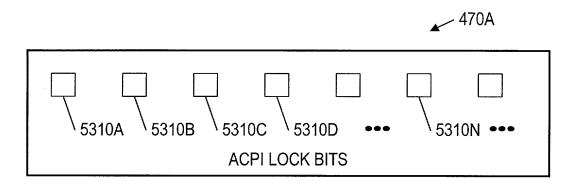


Fig. 42A

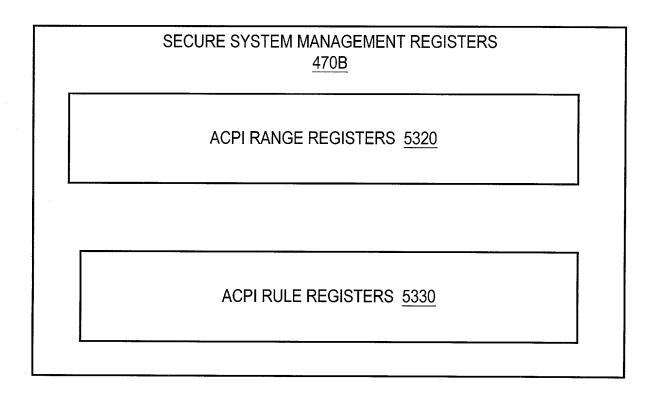


Fig. 42B